Following are the relevant parameters (shown with default values) for enabling the individual trap conditions:

```
[in TRAP/""]
call-log-serv-change-enabled = no
voip-gk-change-enabled = no
wan-line-state-change-enabled = no
```

Parameter	Setting
`call-log-serv-change-enabled`	Enable/disable notification when the call-logging server changes. If the call-logging server index is changed or if the IP address of the active call-logging server is changed, this trap notification sends the following information to the SNMP manager: • The new call logging server index (callLoggingServerIndex) • The IP address of new call logging server (callLoggingServerIPAddress) • The absolute that the server change occurred (sysAbsoluteCurrentTime) (Ascend Trap 38)
`voip-gK-change-enabled`	Enable/disable notification when the registered gatekeeper changes. If a new Gatekeeper is registered with the gateway, a register request (RRQ) message is sent from the gateway to the new gatekeeper. When the gateway receives the admission request (ARQ) message from the new gatekeeper, this notification sends the following information to the SNMP manager: • The new gatekeeper index (voipCfgGkIndex) • The IP address of new gatekeeper (voipCfgGkIpAddress) • The absolute time that the gatekeeper change occurred (sysAbsoluteCurrentTime) (Ascend Trap 39)
`wan-line-state-change-enabled`	Enable/disable notification if the state of an E1 or T1 line changes. This trap sends the following information to the SNMP manager: • The T1 or E1 line interface index (wanLineIfInde) • The line usage (wanLineUsage). This usage is reported as `trunk`, `quiesced`, or `disabled`. • The absolute time that the line state changed (sysAbsoluteCurrentTime) (Ascend Trap 40)

The VoIP MIB (ascend 28)

The VoIP MIB enables network management stations to monitor MultiVoice Gateway operations using SNMP. Attributes in the MIB can be obtained by SNMP Get and Get-Next commands. The MIB uses the following object identifiers for identifying MultiVoice Gateway or MultiVoice Gatekeepers to a network manager:

- voipCfgGroup (voipGroup 1)
- voipCfgGkGroup (voipCfgGroup 1)
- voipCfgGwGroup (voipCfgGroup 2)

The MIB uses the following tables for identifying MultiVoice Gateway and MultiVoice Access Manager functions.

```
voipCfgGkTable OBJECT-TYPE (voipCfgGkGroup 1)
   SYNTAX SEQUENCE OF VoipCfgGkEntry
   ACCESS not-accessible
   STATUS mandatory
   DESCRIPTION A list of entries for H323 network Gatekeeper.
voipCfgGkEntry OBJECT-TYPE (voipCfgGkTable 1)
   SYNTAX VoipCfgGkEntry
   ACCESS not-accessible
   STATUS mandatory
   DESCRIPTION An entry holding information about the Gatekeeper for
   the system.
   INDEX (voipCfgGkIndex)
VoipCfgGkEntry:
   SEQUENCE :
      voipCfgGkIndex-INTEGER
      voipCfgGkStatus-INTEGER
      voipCfgGkIpAddress-IpAddress)
voipCfgGkIndex OBJECT-TYPE ( voipCfgGkEntry 1)
   SYNTAX INTEGER
   ACCESS read-only
   STATUS mandatory
   DESCRIPTION This number uniquely identifies the Gatekeeper.
voipCfgGkStatus OBJECT-TYPE (voipCfgGkEntry 2)
   SYNTAX INTEGER:
      registered(1)
      not_registered(2)
   ACCESS read-only
   STATUS mandatory
   DESCRIPTION This value indicates whether the gateway is registered
   with the Gatekeeper.
voipCfgGkIpAddress OBJECT-TYPE (voipCfgGkEntry 3)
   SYNTAX IpAddress
   ACCESS read-only
   STATUS mandatory
   DESCRIPTION The IP address of the Gatekeeper.
voipCfgGwVpnMode OBJECT-TYPE (voipCfgGwGroup 1)
   SYNTAX INTEGER:
      no (1)
      yes(2)
   ACCESS read-only
   STATUS mandatory
   DESCRIPTION Virtual Private Network Toggle Switch.
```

```
voipCfgGwPktAudioMode OBJECT-TYPE (voipCfgGwGroup 2)
   SYNTAX INTEGER:
      other(1)
      g711_ulaw(2)
      g711_alaw(3)
      g723(4)
      g729(5)
      g723_6_4kps(6)
   ACCESS read-only
   STATUS mandatory
   DESCRIPTION Audio Coder to be used for voice packetization.
```

The voipCfgGwVpnMode and voipCfgGwPktAudioMode objects can be accessed using index 0 because they are separate leaves in the MIB tree.

The voipCfgGkIndex, voipCfgGkCurrent and voipCfgGkIpAddress objects are located in the voipCfgGkTable table. They can be obtained using voipCfgGkIndex as an index.

Sending H.323 call information to SNMP log clients

H.323 call information from MultiVoice Gateways can be collected. This includes the capability to generate start, stop, and call progress records for both VoIP and fax calls.

H.323 call information from MultiVoice Gateways performing VoIP call processing can be sent to SNMP log clients. Each MultiVoice Gateway provides the following H.323 call information:

- Billing start records
- Billing stop records
- Call disconnect records
- Fax start records

Billing start records

A billing start record reports the point in the call where speech communications is established. Start records provide the following information:

Attribute	Specifies
Call ID	The H.323 protocol call ID. This is a unique nonzero number assigned by a MultiVoice Gateway upon receipt of a call, and is used to track all call processing events related to a particular call.
Conference ID	The H.225.0 protocol messaging ID. This is a unique nonzero number assigned by a MultiVoice Gateway upon receipt of a call, and is used to track H.225.0 call setup messages related to a particular call.
Dial time	The time a user spends dialing the destination telephone number. This is the time a MultiVoice Gateway waits to collect the dialed telephone number. This value is zero for calls originating from the LAN.

Attribute	Specifies
Setup time	The time from the moment a user finishes dialing the destination telephone number until the moment the speech is established to the called destination.
Call origin	The IP address used to identify the calling origin. This can be the ingress MultiVoice Gateway or an H.323-compliment terminal.
Remote IP	The IP address used to identify the called destination. This can be the egress MultiVoice Gateway or an H.323-compliment terminal (PC).
Telephone number	The dialed number string entered by the user.
CLID number	The E.164 address associated with the calling origin.
Audio mode	The audio codec used to connect an H.323 call.

Billing stop records

A billing stop record reports the point in the call where speech communications terminates (end points go on-hook). Stop records provide the following information:

Attribute	Specifies
Call ID	The H.323 protocol call ID. This is a unique nonzero number assigned by a MultiVoice Gateway upon receipt of a call, and is used to track all call processing events related to a particular call.
Conference ID	The H.225.0 protocol messaging ID. This is a unique nonzero number assigned by a MultiVoice Gateway upon receipt of a call and is used to track H.225.0 call setup messages related to a particular call.
Connect time	The time from the moment speech is established until the callers hang up (go onhook) normally.
Drop time	The time a call connection is dropped by the WAN or LAN connection, which ever signal is reported first.
Drop reason	The H.323 call drop reason. For normal call termination, the billing stop record reports normalDrop.

Call disconnect records

A call disconnect record is generated whenever a call is not terminated normally (such as when a connection between end points is lost as a result of equipment failure or network failure). Disconnect records provide the following information;

though some information may not be present as depending upon the origin of the call failure:

Attribute	Specifies
Call ID	The H.323 protocol call ID. This is a unique nonzero number assigned by a MultiVoice Gateway upon receipt of a call, and is used to track all call processing events related to a particular call.
Conference ID	The H.225.0 protocol messaging ID. This is a unique nonzero number assigned by a MultiVoice Gateway upon receipt of a call, and is used to track H.225.0 call setup messages related to a particular call.
Dial time	The time a user spends dialing the destination telephone number. This is the time a MultiVoice Gateway waits to collect the dialed telephone number. This value is zero for calls originating from the LAN.
Setup time	The time from the moment a user finishes dialing the destination telephone number until the moment the speech is established to the called destination.
Call origin	The IP address used to identify the calling origin. This can be the ingress MultiVoice Gateway or an H.323-compliment terminal.
Remote IP	The IP address used to identify the called destination. This can be the egress MultiVoice Gateway or an H.323-compliment terminal (PC).
Telephone number	The dialed number string entered by the user.
CLID number	The E.164 address associated with the calling origin.
Audio mode	The audio codec used to connect an H.323 call.
Drop from	The location which disconnected the call, either WAN or LAN.
Drop reason	The H.323 call drop reason. For disconnect reports, this is an incomplete and interrupted call termination reason.

Fax start records

A fax start record is generated whenever a fax answer tone is detected during a VoIP. The fax record provides the following information:

Attribute	Specifies
`Call ID`	The H.323 protocol call ID. This is a unique nonzero number assigned by a MultiVoice Gateway upon receipt of a call, and is used to track all call processing events related to a particular call.
`Conference ID`	The H.225.0 protocol messaging ID. This is a unique nonzero number assigned by a MultiVoice Gateway upon receipt of a call and is used to track H.225.0 call setup messages related to a particular call.
`Modulation type`	The fax modulation type detected by the MultiVoice Gateway (such as V.21, V.27, V.29, V.17, etc.)
Speed	The transmission speed, modulation rate, detected for this fax transmission by the MultiVoice Gateway (such as 2400, 4800, 7200, etc.)

Note Fax records are generated for T.38 fax transmissions.

H.323 disconnect reasons

H.323 disconnect reasons have been added to `disconnect-reason-type.mibdef` for the Ascend disconnect type. Reported disconnect reasons for standard and nonstandard call termination are recorded in the following table.

Call drop reason	Call drop code	Specifies
DIS_H323_DROP_REASON_NULL	500	Call drop reason not available
DIS_H323_DROP_REASON_NORMAL	501	Normal disconnect (caller hung up)
DIS_H323_DROP_REASON_DEST_BUSY	502	Called destination busy
DIS_H323_DROP_REASON_DEST_UNREACHABLE	503	Called destination unreachable
DIS_H323_DROP_REASON_REJECT	504	Call rejected by TAOS
DIS_H323_DROP_REASON_WAN_FAILURE	505	WAN failure, egress MultiVoice Gateway could not connect the call

Call drop reason	Call drop code	Specifies
DIS_H323_DROP_REASON_GATEWAY_RESOURCES	506	Egress MultiVoice Gateway could not process the call
DIS_H323_DROP_REASON_NO_BANDWIDTH	507	Sufficient bandwidth not available on the WAN for this call
DIS_H323_DROP_REASON_GW_NOT_REGISTERED	508	Egress MultiVoice Gateway is currently unregistered with the MVAM
DIS_H323_DROP_REASON_INVALID_PIN	509	Caller entered an invalid PIN
DIS_H323_DROP_REASON_INVALID_DNIS	510	Caller dialed invalid number for called destination
DIS_H323_DROP_REASON_NO_LAN_ANSWER	511	A LAN connection was not available
DIS_H323_DROP_REASON_STATE_MACHINE	512	Call state machine on MultiVoice Gateway could not advance
DIS_H323_DROP_REASON_NO_LAN_DISCONNECT	513	The WAN dropped the connection
DIS_H323_DROP_REASON_FEGW_CAUSE_CODE	514	The egress MultiVoice Gateway dropped the connection
DIS_H323_DROP_REASON_MAX_PIN_ATTEMPTS	515	The caller failed to authenticate on all attempts to enter the PIN
DIS_H323_DROP_REASON_CODER_DENIED	516	The MultiVoice Gateway could not negotiate an audio codec selection with the far-end gateway

NavisAccess™ support for VoIP call reporting

Basic VoIP call reporting using NavisAccess™ includes the capability to generate start records, stop records, and call progress records for both VoIP and fax calls. These

records allow NavisAccess™ to monitor gateway resource usage and provide information to create billing records. Each VoIP call can generate two or more records.

Start records

A start record reports the point in the call where a speech communications is established. Start records can provide the following information:

Attribute	Specifies
Ascend-Call-Direction	Direction of the call between the gateway and PSTN. The reported values are Ascend-Call-Direction-Incoming (0) and Ascend-Call-Direction-Outgoing (1). (Ascend Trap 48)
NAS-Port	Encoded NAS port used for this call. (RFC Trap 5)
NAS-Port-Type	Encoded NAS port used for this call. The value 7 for this attribute identifies a VoIP call. (RFC Trap 61)
NAS-IP-Address	NAS IP address associated with this call. (RFC Trap 4)
Session-Id	NAS session index recorded in the session table for this call. (RFC Trap 44)
Ascend-Modem-PortNo	DSP/modem port allocated for processing this call. This value is part of the resource count information, and is repeated each time it is allocated for a call. (Ascend Trap 120)
Ascend-Modem-SlotNo	Slot where the DSP/modem card associated with the reported Ascend-Modem-PortNo is located. This value is part of the resource count information, and is repeated each time it is allocated for a call. (Ascend Trap 121)
Ascend-Modem-ShelfNo	Shelf where DSP/modem card allocated for processing this call is installed. This is part of the resource count information, and is repeated each time it is allocated for a call. (Ascend Trap 122)
Called-Station-Id (DNIS)	Dialed number string reported by the gateway for the called destination. (RFC Trap 30)
Ascend-Dialed-Number	Dialed number string used by the gateway to complete the call. (Ascend Trap 24)
Service-Type	Requested type of service, the value of the Type of Service byte, for this call. (RFC Trap 6)
Ascend-H323-Destination-NAS-ID	NAS IP address used to route the call to the connecting gateway. (Ascend Trap 22)
Ascend-H323-Gatekeeper-IP	IP address of the Gatekeeper used to route the call. The gateway is registered with this gatekeeper. (Ascend Trap 19)
Ascend-Global-Call-Id	IP address used by the gatekeeper to identify the connecting gateway for this call. (Ascend Trap 20)

Attribute	Specifies
Ascend-H323-Conference-ID	IP address used to identify the called destination. (Ascend Trap 21)
Ascend-H323-Presession-Time	Time from the moment the caller finishes dialing the destination telephone number until the moment the speech path is established to the called destination. (Ascend Trap 198)
Ascend-H323-Dialed-Time	Time the user spends dialing the destination telephone number. This value is zero for a call originating from the WAN. (Ascend Trap 23)
Ascend-Session-Type	Audio codec used for processing the call. (Ascend Trap 18)

Stop records

A stop record is generated at the moment when MultiVoice begins to tear down the speech path or when an incoming call to a gateway fails to connect. A stop record can contain the following information:

Attribute	Specifies
Acct-Session-Time	Time from the moment the speech path is established to the called destination until the moment MultiVoice begins to tear down the speech path. (RFC Trap 46)
Ascend-Connect-Progress	A number that represents the call connect state at the time the call was terminated. (Ascend Trap 195)
Ascend-Disconnect-Cause	A number that reports the H.323 call disconnection reason. (Ascend Trap 196)
Ascend-H323-Inter-Arrival-Jitter	Estimated interarrival jitter for voice packets received by a gateway. (Ascend Trap 25)
Ascend-Dropped-Octets	The number of voice frames (in bytes) dropped by a gateway during call processing. (Ascend Trap 26)
Ascend-Dropped-Packets	Number of voice packets dropped by a gateway during call processing. (Ascend Trap 26)
Acct-Input-Octets	Number of voice frames (in bytes) received by a gateway during this call. (RFC Trap 42)
Acct-Input-Packets	Number of voice packets received by a gateway during this call. (RFC Trap 47)
Acct-Output-Octets	Number of voice frames (in bytes) sent by a gateway during this call. (RFC Trap 43)
Acct-Output-Packets	Number of voice packets sent by a gateway during this call. (RFC Trap 48)

Call progress records

A call progress record can be generated during a VoIP call when a change in resource occurs for a fax or transparent modem call. For fax calls, this record includes the modem speed and modulation. A progress message contains all the information included in a start record.

NavisAccess™ support for RTP payload information

The RTP QoS statistics generated are obtainable periodically, through a polling parameter. RTP QoS periodic statistics (such as end-of-call statistics) are sent to the IPDC protocol (this function is not dependent upon the enabling of either RTP QoS polling or Call Logging).

Supported codecs for this feature are limited to G.711 and G.729 on a MultiVoice Gateways. RTP QoS information passed onto the Call Logging Server is enhanced in this feature to offer a good perspective of the QoS.

The RTP QoS feature can be observed in three factions: Polling, Call Logging, and IPDC.

- In polling, a `voip` profile parameter `rtpqos-polling-enable` can be activated so the i960 processor requests periodic statistics of the SARMs.
- In call logging, for each active call these statistics will be returned every 60 seconds, and once received, will forward the statistics to the call logging mechanism.
- For IPDC, one end-of-call statistic, Estimated Jitter, will be available for the IPDC signaling layer.

Note This feature is available only on a MultiVoice Gateway configured with MultiDSP cards.

TAOS collects information periodically during the voice call—the general information content is described in Table 6-1.

The RTP statistics set, sent to the STOP packet's call logging server, is enhanced through the addition of attributes into that packet. TAOS collects periodic information during voice calls. Table 6-1 is a description of this QoS information content.

Table 6-1. Qos Information

Direction	**LocalGW - RemoteGW**			**RemoteGW - LocalGW**		
Info (Units)						
	Sent	Lost	Late	Sent	Lost	Late
Packets(N)	X	X	X	X	X	X
Bytes (N)			Applies to both			
* Jitter (ms)		X			X	
* Round Trip Delay (ms)			Applies to both			
Silence Detect (% of Packets)		X			X	

Note Maximum observed value, minimum observed value, average and standard variance are provided in the STOP packet.

The implementation of the STOP packet information generates a new MIB; ASCEND-RTP-QOS-STATS-MIB. You can use this MIB to extract QoS statistics for an active VoIP (RTP) call.

For call logging and IPDC, N/A is appropriate.

To generate RTP QoS statistics, enable the `rtpqos-polling-enable` parameter in the `voip` profile.

Parameter	**Setting**
`rtpqos-polling-enable`	Setting this to yes generates RTP QoS statistics periodically, through a polling parameter. RTP QoS periodic statistics (such as end-of-call statistics) are sent to the IPDC protocol (this function is not dependent upon the enabling of either RTP QoS polling or Call Logging). Default is no. **Note** This parameter is only applicable when the `packet-audio-mode` parameter is set to G.711 or G.729.

Call logging STOP packet

The Call Logging STOP Packet contains the attributes given in the tables below:

Option	**Specifies**
`Ascend-Rtp-Local-Jitter-Minimum`	Minimum jitter measured at local RTP receiver
`Ascend-Rtp-Local-Jitter-Maximum`	Maximum jitter measured at local RTP receiver
`Ascend-Rtp-Local-Jitter-Mean`	Average jitter measured at local RTP receiver

Option	Specifies
Ascend-Rtp-Local-Jitter-Variance	Variation in jitter measured at local RTP receiver
Ascend-Rtp-Local-Delay-Minimum	Minimum round trip delay measured at local RTP transmitter
Ascend-Rtp-Local-Delay-Maximum	Maximum round trip delay measured at local RTP transmitter
Ascend-Rtp-Local-Delay-Mean	Average round trip delay measured at local RTP transmitter
Ascend-Rtp-Local-Delay-Variance	Variation in round trip delay measured at local RTP transmitter
Ascend-Rtp-Local-Packets-Sent	Total number of packets transmitted by local RTP transmitter
Ascend-Rtp-Local-Packets-Lost	Total number of packets failed to arrive at local RTP transmitter
Ascend-Rtp-Local-Packets-Late	Total number of packets arrived late at local RTP transmitter
Ascend-Rtp-Local-Silence-Sent	Total number of bytes transmitted by local RTP transmitter
Ascend-Rtp-Local-Silence-Percent	Percentage silence measured at local RTP transmitter

Remote RTP transmitter and receiver

The following are statistics regarding Remote RTP Transmitter and Receiver:

Option	Specifies
Ascend-Rtp-Remote-Jitter-Minimum	Minimum jitter measured at Remote RTP receiver
Ascend-Rtp-Remote-Jitter-Maximum	Maximum jitter measured at Remote RTP receiver
Ascend-Rtp-Remote-Jitter-Mean	Average jitter measured at Remote RTP receiver
Ascend-Rtp-Remote-Jitter-Variance	Variation in jitter measured at Remote RTP receiver
Ascend-Rtp-Remote-Delay-Minimum	Minimum round trip delay measured at Remote RTP transmitter
Ascend-Rtp-Remote-Delay-Maximum	Maximum round trip delay measured at Remote RTP transmitter
Ascend-Rtp-Remote-Delay-Mean	Average round trip delay measured at Remote RTP transmitter

Option	Specifies
Ascend-Rtp-Remote-Delay-Variance	Variation in round trip delay measured at Remote RTP transmitter
Ascend-Rtp-Remote-Packets-Sent	Total number of packets transmitted by Remote RTP transmitter
Ascend-Rtp-Remote-Packets-Lost	Total number of packets failed to arrive at Local RTP transmitter
Ascend-Rtp-Remote-Packets-Late	Total number of packets arrived late at Local RTP transmitter
Ascend-Rtp-Remote-Silence-Sent	Total number of bytes transmitted by Remote RTP transmitter
Ascend-Rtp-Remote-Silence-Percent	Percentage silence measured at Remote RTP transmitter

End-of-call statistics

The end-of-call statistics are supported by two IPDC messages—the RCR and the ACR message:

RCR Message

Tag 0 x 99 (Estimated Latency): This tag is now added. It contains a value estimating the latency (delay) measured during the call.

Tag 0 x A3 (Estimated Jitter): This tag is was already included with the end-of-call statistics, but its value is always set to 0. It contains a value estimating the jitter measured during the call.

ACR Message

Tag 0 x 99 (Estimated Latency): This tag is now added. It contains a value estimating the latency (delay) measured during the call.

Tag 0 x A3 (Estimated Jitter): This tag is was already included with the end-of-call statistics, but its value is always set to 0. It contains a value estimating the jitter measured during the call.

Reporting cause codes to MVAM

The reporting capabilities of a MultiVoice Gateway include the Q.931 cause code or H.225 Release Complete reason in the data reported to the MultiVoice Access Manager (MVAM) in a Drop Request (DRQ) message.

Release codes

There are two types of release codes that can be reported when a VoIP call is terminated, either Q.931 Cause codes or H.225 Release Complete Reason codes. MultiVoice uses the event definitions in the H.323 stack to determine which release code gets reported in the DRQ.

The MultiVoice Gateway extracts the Q.931 Cause code or H.225 Release Complete reason from H.225 Connection object (release complete message); then reports the release code as part of the nonStandardData byte sent to MVAM in the DRQ message.

When reporting call release codes, MultiVoice reports:

- The Q.931 Cause code when the event that terminates the VoIP call is related to a call progress error on active calls
- The H.225 Release Complete reason code when the event that terminates the VoIP call is related to a call admission error

For TAOS 5.0Ap23, the Q.931 Cause codes listed in Table 6-2 are reported by MultiVoice Gateways as call release codes.

Table 6-2. Reported Q.931 Cause codes

H.323 Cause code	Code
H323_Call_Rejected	256
H323_Call_No_Answer	257
H323_Call_Busy	258
H323_Call_Failed	259
H323_Call_No_Resources	260
H323_Call_No_Bandwidth	262
H323_Call_No_Destination	163
H323_Call_No_Gatekeeper	164
H323_Call_Bad_Format	165
H323_Call_Not_Registered	166
H323_Call_Network_Failed	167
H323_Call_Unassigned_Num	168
H323_Call_Dest_OutofOrder	169
H323_Call_Invalid_Pin	170
H323_Call_Invalid_Dnis	171
H323_Call_Pin_Required	172
H323_Call_2Dnis_Required	173
H323_Call_PinAnd2Dnis_Required	174

For TAOS 5.0Ap23, the H.225 Release Complete reason codes found in Table 6-3 are reported by MultiVoice Gateways as call release codes.

Table 6-3. Reported H.225 Cause codes

H.225 Reason Complete	Code
H225_Idle	100
H225_RAS_Reject	112
H225_RAS_Drop	113

Reporting Q.931 messages

Q.931+ message trace information displayed in English language format. Previously, diagnostic and status information was displayed in hexadecimal format, which provides no intuitive information as to message meanings.

The diagnostic and status information that is displayed in English language format includes the following:

- Q.931 call progress events
- Layer 2 and Layer 3 transport events
- Initialization and data transport errors

Modifications to the ss7asg command

The ss7asg debug-level command output reports TUNL message statistics when entered as follows:

```
admin> ss7asg -s
```

The -s option of the ss7asg command provides an English language summary of SS7 signaling activity for a MultiVoice Gateway. A new debug option for dumping call information elements (IE) are available and added as part of this enhancement. TAOS 9.0 modifies the ss7asg debug command to include the following options:

Options	Specifies
`-i`	Display the SS7 interface ID map
`-m`	Show all MCBs (ME control blocks)
`-n`	Show all NLCBs (Layer 3 call blocks)
`-s`	Show SS7 interface statistics
`-r`	Reset SS7 signaling layer statistics

To set the diagnostics level for the ss7asg command, use the following `Diag` command to assign the appropriate debug level:

```
diag ss7asg level
```

Debug level	Specifies
0x00	Diagnostic output is disabled. No debugging information is collected.
0x01	Report errors only. Collect only high level error information as errors occur.
0x02	Record Layer 3 events and state changes. The Layer 3 state transitions are displayed as they happen.
0x04	Record call control events. Collect in session logs.
0x08	Collect decoded information elements (IE) for each SS7 call.
0x10	Show detailed debugging traces. Collect full session logs, including low-level processing information.
0x20	Enable code trace for debugging
0x40	Record Layer 3 packet information
0x80	Collect call control primitives
0x100	Collect signaling link event information
0x200	Show memory allocation/deallocations for TAOS unit processing of SS7 calls.

Displaying extended information

Extended information elements contain processing details about ASG call processing. Setting debug level 0x08 displays the following information elements decoded (nonhexadecimal) format:

- Bearer cap
- Called Party number
- Calling Party number
- Cause value
- Call state
- Channel identification
- Call reference

The following example illustrates the output of the `ss7nmi -m` command, reporting the TUNL messaging statistics:

```
tnt-176> ss7asg -s
SS7 Signaling Gateway interface statistics:
        Initialized successfully:               No
        Interface state:                        Disabled
        Diagnostic level:                       0
Initialization Errors:
        Number of errors in initialization:     0
        Memory pools:                           0
        Mailboxes:                              0
```

```
Signaling Layer:
        Number of SETUP requests from:          L2: 0       CC: 0
        Number of CONNECT to ASG:               0
        Number of CONNECT_ACK from ASG:         0
        Number of SETUP rejected from:          L3: 0       CC: 0
        Number of DISCONNECT requests from:     L2: 0       CC: 0
        Number of REGISTRATION to ASG:          0
        Number of REGISTRATION_ACK from ASG:    0
        Number of SERVICE recv:                 0
        Number of SERVICE_ACK xmit:             0
        Number of DL_REL_IND from L2:           0
        Number of DL_EST_IND from L2:           0
        Number of T303 expiry events:           0
        Number of T305 expiry events:           0
        Number of T308 expiry events:           0
        Number of BC Resp without matched NLCB: 0
        Last L3 counters reset timestamp:       [09/27/2000 08:17:54]
Data Transport Layer:
        Number of link fail-overs:              0
        Number of persistent errors:            0
        Last error:                             No Error
        Last error status change timestamp:     [01/01/1990 00:00:00]
```

Reporting call failures in cause codes

The MultiVoice Gateway reports the call progress cause code in the billing Disengage Request (DRQ). This cause code is recorded in call detail records (CDRs) and in debug information so that all necessary information can be examined to determine the precise point of failure.

Background

Historically, many ISDN switches sent a release complete message instead of the call progress message that contained the call failure reason. The message oftentimes reported ambiguous and misleading call failure information.

The real reason of failure was contained in the call progress message, but was ignored. The call progress message contained a CAUSE field that includes the type of call failure (for example, `Invalid Number Format`).

Implementation Details

To more accurately reflect the exact cause of call failure, the following has been implemented:

- When a Call Progress message contains a Progress Indicator of 8 from the PSTN, the value of the Q.391 cause code is captured. The reason indicates why the call failed (for example, `Invalid Number Format`).
- A progress cause code is a embedded in the DRQ message, which is recorded by the Gatekeeper (for example, MVAM).

- The Gatekeeper includes the new cause code information in a new field of the call detail record (CDR). Look at the release cause code of the CDR to determine if a problem occurred during the processing of the call.
- The cause code information is displayed using h323debug.

Calculating and reporting packet jitter

Jitter calculation on the StrongARM (SARM) processor for reporting RTP packet transmissions is available in TAOS 5.0Ap23. The packet jitter on a MultiVoice Gateway is reported to both the Media Gateway Controller (SoftSwitch) for IP Device Control (IPDC) protocol packets and to NavisAccess™ administration systems.

The jitter calculation provides an estimate of the statistical variance of the RTP data packet interarrival time, measured in timestamp units and expressed as an unsigned integer. The interarrival jitter is defined to be the mean deviation (smoothed absolute value) of the difference in packet spacing at the receiver compared to the sender for a pair of packets. As the control DSP accepts packets from the i960 processor shared memory interface, jitter is calculated using the formula defined in RFC 1889, *RTP: A Transport Protocol for Real-Time Applications*, (Jan. 1996), IETF, as illustrated:

```
jitter += (1/16)*(d-(jitter))
```

The results of this equation returns the equivalent of the difference in the relative transit time for the two packets; the relative transit time is the difference between a packet's RTP timestamp and the receiver's clock at the time of arrival, measured in the same units. Since all time calculations on MultiVoice Gateways are executed using a fixed point system, the jitter calculation is implemented using the following modified version of the formula specified by RFC 1889:

```
jitter += (d - (jitter + 8) >> 4);
```

In this case, the difference (d) is the difference between the current transit time and the previous transit time, as defined in RFC 1889. This value is maintained for each Slave DSP.

Transit time is calculated by calculating the time difference between two consecutive packets, and subtracting the difference in RTP timestamps. The values are reported to the i960 through the Query Call Stats message response, the 32 bit jitter response is added to the end of message as first word, upper 16 bits, second word, lower 16 bits. The value is the number of 125us ticks.

Q.931 messaging for SS7 V.110 calls

The feature adds Q.931 messaging support for requesting V.110 bearer capability for Signal System 7 (SS7) calls. A second octet in the call setup message information element is sent by a protocol control gateway (PCG). When a PCG, such as Lucent SoftSwitch, includes the Q.931 information element in the call setup message, the information element enables asynchronous transfer mode and disables in-band negotiation.

For calls requiring V.110 bearer capability, the PCG generates a Q.931 call setup message requesting bearer capability at one of the following unrestricted

adaptation rates, in bits-per-second (bps), supported by MAX TNT or APX 8000 units:

- 2400bps to 64Kbps
- 4800bps to 64Kbps
- 9600bps to 64Kbps
- 19200bps to 64Kbps
- 38400bps to 64Kbps

Supported Q.931 bearer capability requests

The call type is set in octet 5 of the Q.931 call setup message sent from the SoftSwitch to the TAOS unit. The adaptation rate is retrieved from the user rate in octet 5a of the Q.931 call setup message.

The following table lists the TAOS-supported bearer capability requests that can be assigned to Octet 5 of the Q.931 setup message by the PCG for SS7 call processing:

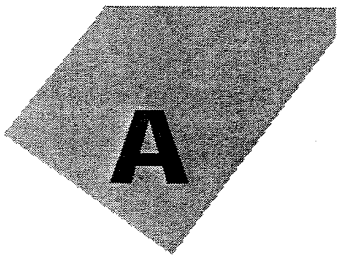
Request	Specifies
0x04 0x03 0x80 0x90 0xa0	Speech bearer capability.
0x04 0x04 0x88 0x90 0x21 0xc3	V.110 bearer capability with 2400bps to 64Kbps unrestricted adaptation.
0x04 0x04 0x88 0x90 0x21 0xc5	V.110 bearer capability with 4800bps to 64Kbps unrestricted adaptation.
0x04 0x04 0x88 0x90 0x21 0xc8	V.110 bearer capability with 9600bps to 64Kbps unrestricted adaptation.
0x04 0x04 0x88 0x90 0x21 0xcb	V.110 bearer capability with 19200bps to 64Kbps unrestricted adaptation.
0x04 0x04 0x88 0x90 0x21 0xcd	V.110 bearer capability with 38400bps to 64Kbps unrestricted adaptation.

Octet 5a information element

When the Q.931 call setup message sent by the PCG requests V.110 bearer capability, the following values must be assigned to Octet 5a to enable asynchronous transfer mode and suspend in-band call signaling on a TAOS unit for the duration of the SS7 call.

Bit #	Value	Description
Bit 7	1	Enable asynchronous data mode for this call
Bit 6	0	Disable in-band negotiation

MultiVoice Packet Processing

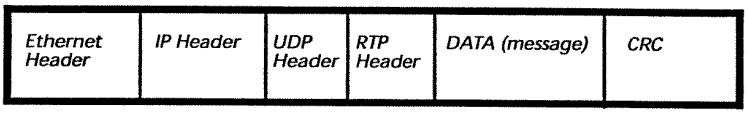


MultiVoice H.323 voice and data transmissions utilize User Datagram Protocol (UDP) packetting for processing voice and RAS channel messages. The Real-time Transfer Protocol (RTP) packets, which contain the voice data, run on top of UDP.

MultiVoice packet format

The size of each MultiVoice packet is determined by the number of audio frames contained in each RTP packet plus the size of the respective headers required to construct the Ethernet frame. Each component of the Ethernet frame include the following elements:

Figure A-1. MultiVoice packet format



where:

Table A-1. Multivoice packet descriptions (Page 1 of 2)

Element	Size	Description
Ethernet Header	18 bytes	This header contains the source and destination MAC addresses (station addresses) used for the data link between two gateways.
IP Header	20 bytes	This header contains source and destination IP addresses. If MultiVoice packets become fragmented at the IP transport layer, multiple datagrams are generated and assigned sequence numbers so they can be reassembled at the destination gateway.
UDP Header	8 bytes	This header contains the source and destination ports as well as the sequence number of the packet.

Table A-1. Multivoice packet descriptions (Page 2 of 2)

Element	Size	Description
RTP Header	12 bytes	This header contains timestamping and synchronization information for proper reassembly of data at the destination gateway.

Packet sizes by audio codec

The RTP packet header contains a time stamp and sequence number used to reconstruct the voice message. The header size is fixed at 12 bytes. The size of the packet data will vary, depending upon the type of audio codec defined for `packet-audio-mode` parameter.

Table A-2 provides information on the RTP packet sizes and processing times by audio codec.

Table A-2. RTP packet sizes (Page 1 of 5)

Audio codec	Number of voice frames	RTP packet size (includes RTP header)	Ethernet frame size	Bits per second	Packets per second
G.711	1 @ 5ms ea.	52 Bytes	98 Bytes	156800	200
	2 @ 5ms ea.	92 Bytes	138 Bytes	110400	100
	3 @ 5ms ea.	132 Bytes	178 Bytes	94933.33	66.667
	4 @ 5ms ea.	172 Bytes	218 Bytes	87200	50
	5 @ 5ms ea.	212 Bytes	258 Bytes	82560	40
	6 @ 5ms ea.	252 Bytes	298 Bytes	79466.67	33.333
	7 @ 5ms ea.	292 Bytes	338 Bytes	77257.143	28.571
	8 @ 5ms ea.	332 Bytes	378 Bytes	75600	25
	9 @ 5ms ea.	372 Bytes	418 Bytes	74311.11	22.222
	10 @ 5ms ea.	412 Bytes	458 Bytes	73280	20

Table A-2. RTP packet sizes (Page 2 of 5)

Audio codec	Number of voice frames	RTP packet size (includes RTP header)	Ethernet frame size	Bits per second	Packets per second
G.723.1 @ 5.3 Kbps	1 @ 30 ms ea.	32 Bytes	78 Bytes	20800.000	33.333
	2 @ 30 ms ea.	52 Bytes	98 Bytes	13066.667	16.667
	3 @ 30 ms ea.	72 Bytes	118 Bytes	10488.889	11.111
	4 @ 30 ms ea.	92 Bytes	138 Bytes	9200.000	8.333
	5 @ 30 ms ea.	112 Bytes	158 Bytes	8426.667	6.667
	6 @ 30 ms ea.	132 Bytes	178 Bytes	7911.111	5.556
	7 @ 30 ms ea.	152 Bytes	198 Bytes	7542.857	4.762
	8 @ 30 ms ea.	172 Bytes	218 Bytes	7266.667	4.167
	9 @ 30 ms ea.	192 Bytes	238 Bytes	7051.852	3.704
	10 @ 30 ms ea.	212 Bytes	258 Bytes	6880.000	3.333

Table A-2. RTP packet sizes (Page 3 of 5)

Audio codec	Number of voice frames	RTP packet size (includes RTP header)	Ethernet frame size	Bits per second	Packets per second
G.723.1 @ 6.4 Kbps	1 @ 30 ms ea.	36 Bytes	82 Bytes	21866.667	33.333
	2 @ 30 ms ea.	60 Bytes	106 Bytes	14133.333	16.667
	3 @ 30 ms ea.	84 Bytes	130 Bytes	11555.556	11.111
	4 @ 30 ms ea.	108 Bytes	154 Bytes	10266.667	8.333
	5 @ 30 ms ea.	132 Bytes	178 Bytes	9493.333	6.667
	6 @ 30 ms ea.	156 Bytes	202 Bytes	8977.778	5.556
	7 @ 30 ms ea.	180 Bytes	226 Bytes	8609.524	4.762
	8 @ 30 ms ea.	204 Bytes	250 Bytes	8333.333	4.167
	9 @ 30 ms ea.	228 Bytes	274 Bytes	8118.519	3.704
	10 @ 30 ms ea.	252 Bytes	298 Bytes	7946.667	3.333

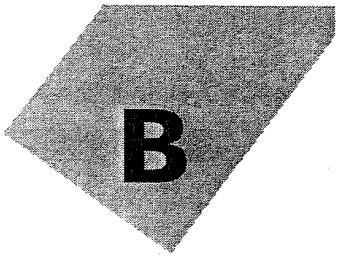
Table A-2. RTP packet sizes (Page 4 of 5)

Audio codec	Number of voice frames	RTP packet size (includes RTP header)	Ethernet frame size	Bits per second	Packets per second
G.728	1 @ 5ms ea.	22 bytes	68 bytes	108800.00	200
	2 @ 5ms ea.	32 bytes	78 bytes	62400.000	100
	3 @ 5ms ea.	42 bytes	88 bytes	46933.333	66.667
	4 @ 5ms ea.	52 bytes	98 bytes	39200.000	50.000
	5 @ 5ms ea.	62 bytes	108 bytes	34560.000	40.000
	6 @ 5ms ea.	72 bytes	118 bytes	31466.667	33.333
	7 @ 5ms ea.	82 bytes	128 bytes	29257.143	28.571
	8 @ 5ms ea.	92 bytes	138 bytes	27600.000	25.000
	9 @ 5ms ea.	102 bytes	148 bytes	26311.111	22.222
	10 @ 5ms ea.	112 bytes	158 bytes	25280.000	20.000
G.729A	1 @ 10ms ea.	22 bytes	68 bytes	54400	100
	2 @ 10ms ea.	32 bytes	78 bytes	31200	50
	3 @ 10ms ea.	42 bytes	88 bytes	23466.67	33.333
	4 @ 10ms ea.	52 bytes	98 bytes	19600	25
	5 @ 10ms ea.	62 bytes	108 bytes	17280	20
	6 @ 10ms ea.	72 bytes	118 bytes	15733.33	16.667
	7 @ 10ms ea.	82 bytes	128 bytes	14628.571	14.286
	8 @ 10ms ea.	92 bytes	138 bytes	13800	12.5
	9 @ 10ms ea.	102 bytes	148 bytes	13155.56	11.111
	10 @10ms ea.	112 bytes	158 bytes	12640	10

Table A-2. RTP packet sizes (Page 5 of 5)

Audio codec	Number of voice frames	RTP packet size (includes RTP header)	Ethernet frame size	Bits per second	Packets per second
Full-rate GSM	1 @ 20ms ea.	45 bytes	91 bytes	22750	50
	2 @ 20ms ea.	78 bytes	124 bytes	24800	25
	3 @ 20ms ea.	111 bytes	157 bytes	20924.96	16.66
	4 @ 20ms ea.	144 bytes	190 bytes	19000	12.5
	5 @ 20ms ea.	177 bytes	223 bytes	17840	10
	6 @ 20ms ea.	210 bytes	256 bytes	17066.66	8.33
	7 @ 20ms ea.	243 bytes	289 bytes	16514.28	7.14
	8 @ 20ms ea.	274 bytes	320 bytes	16000	6.25
	9 @ 20ms ea.	299 bytes	345 bytes	15333.33	5.55
	10 @ 20ms ea.	342 bytes	388 bytes	15520	5

Determining Jitter Buffer Size



The dynamic jitter buffer size is a function of:

- RTP packet duration (in milliseconds) for the selected audio codec
- Total RTP packets as defined by the Initial-Jitter-Buffer-Size and Max-Jitter-Buffer-size parameters

Dynamic jitter buffer size is derived by multiplying the values assigned to the `initial-jitter-buffer-size` and `max-jitter-buffer-size` parameters, respectively, by *packet duration*. Packet duration is the total playout time, in milliseconds, for the speech frames contained in a single RTP packet:

initial-jitter-buffer-size	x	*Packet Duration (ms)*
max-jitter-buffer-size	x	*Packet Duration (ms)*

For example, in fixed mode, if `initial-jitter-buffer-size = 5`, and an in-coming call used the G.711 codec with one audio frame per packet, which has a packet duration of 5ms, then:

5 (Packets) x 5ms/packet = 25ms (jitter buffer length)

The instantaneous jitter buffer size for the VoIP call is 25ms. If a second in-coming call used the G.729(A) codec, and had five audio frames per packet, with a packet duration of 50ms, then the instantaneous jitter buffer size for this subsequent call is 250ms.

Dynamic jitter buffers

The following tables contain the calculated dynamic jitter buffers for a single call, by supported audio codec.

Table B-1. Jitter buffer length (in milliseconds) for the G.711 audio codec (Page 1 of 2)

Jitter[a] buffer packets	Packet duration (ms), for one to 10 audio frames per RTP packet using the G.711 codec									
	1 frame @5ms	2 frames @10ms	3 frames @15ms	4 frames @20ms	5 frames @25ms	6 frames @30ms	7 frames @35ms	8 frames @40ms	9 frames @45ms	10 frames @50ms
1	5	10	15	20	25	30	35	40	45	50
2	10	20	30	40	50	60	70	80	90	100